CIAC Threat Update

Paul Krystosek, PhD
DOE-CIAC
Outreach and Assessment

U.S. Department of Energy CIAC Computer Incident Advisory Capability

Disclaimer LLNL

CIAC is the U.S. Department of Energy's Computer Incident Advisory Capability. Established in 1989, shortly after the Internet Worm, CIAC provides various computer security services to employees and contractors of the DOE, such as:

- Incident Handling consulting
- Computer Security Information
- On-site Workshops
- White-hat Audits

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.

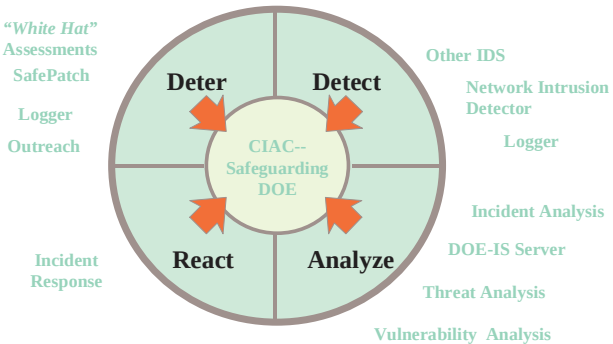
U.S. Department of Energy CIAC Computer Incident Advisory Capability

Overview

- Current threats
- Anticipated threats
- Countermeasures
- Research project ideas

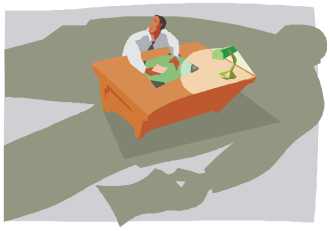
U.S. Department of Energy CIAC Computer Incident Advisory Capability

DOE-CIAC



U.S. Department of Energy CIAC Computer Incident Advisory Capability

Current Threats



- Insider
- Outsider who just got in
- Malicious code
- Unpatched vulnerability
  - Out of the box system
  - Legacy application, instrument w/embedded
- Newly discovered vulnerability
- Unprotected passwords
- Lack of awareness

U.S. Department of Energy CIAC Computer Incident Advisory Capability

Anticipated Threats

- Mobile code
- Mobile workers
- Wireless
- Bigger, faster, smarter, meaner

U.S. Department of Energy CIAC Computer Incident Advisory Capability

Mobile Code

- Probably not amenable to methods used for virus/malicious code checking
- Signing is nice, but… would you trust it
- What will it mean to use it wisely?

Mobile Workers

- The worker is not the threat, per se
- How to accommodate working from home or on travel
  - Authentication
  - Access
  - Resources
  - Secure mobile/remote computer
  - <insert plug for upcoming whitepaper here>

Wireless

- How does the use of wireless devices affect security?
- Potential vulnerabilities
  - Signal capture
  - Unauthorized “connection” to the net
  - “Out of the box” problems
  - <insert plug for upcoming whitepaper here>

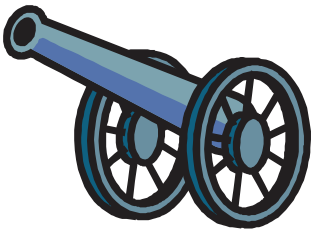
U.S. Department of Energy CIAC Computer Incident Advisory Capability

How Does Moore’s Law Affect Security?

- The Bad Side
  - Faster computers and networks
    - Bigger DDoS scenarios
    - Wider, smarter scans
    - Crack
- The Good Side
  - Faster computers and networks
    - Better IDS, virus detection, firewalls

U.S. Department of Energy CIAC Computer Incident Advisory Capability

- What must we do to improve computer security?
  - Complete the information cycle
  - Nullify the hackers' advantage



U.S. Department of Energy CIAC Computer Incident Advisory Capability

CIAC Input/Output

- CIAC gathers a tremendous amount of data
- What information compiled from that data will make sites' computer security better?
- We currently provide
  - Rose's Bad List
  - Alerts and bulletins
  - Summary data (how many scans, compromises…)
- What else can we do?
  - Link charts

U.S. Department of Energy CIAC Computer Incident Advisory Capability

Hackers' Have the Advantage

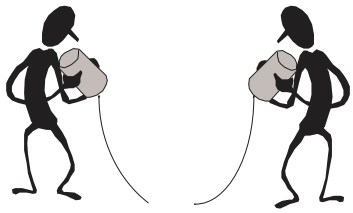
- **Communication**
  - **Publications, web sites, IRC, chat**
- **Surprise**
  - **They can choose from among millions of potential victims and thousands of exploits**
- **Ethics**
  - **They don't need no stinking ethics**

The Public's Disadvantage

- **Communication**
  - **Hacked sites often don't want to talk about it**
- **Surprise**
  - **We have to protect all those millions of systems against all those thousands of exploits**
  - **Too busy/unable to patch all vulnerabilities**
- **Ethics**
  - **Much as we'd like, we can't/shouldn't retaliate**

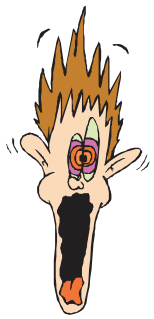
Be More Like a Hacker?

- **Communication**
  - Find a way to get the word out on current activity
  - Distinguish routine from really important
  - Don't ignore the routine
  - Stay in touch
    - Venues like this one
    - DOE SLCCC TWG
  - Report, compile, share



Don't be Surprised

- **Surprise**
  - If we communicate there will be fewer surprises
  - Make time to patch
  - Intrusion detection
    - <insert ad for NID here>
    - DOE security tools purchase
  - Automate patching process
    - <insert ad for SafePatch here>

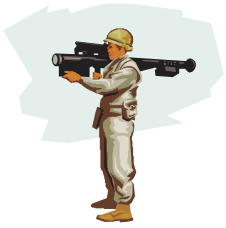


Ethics

- **Hackers**
  - **Instill ethics in them ☺**
  - **Public pressure**

Ethics

- **Find ways to ethically retaliate**
  - **Don't hit the wrong target**
  - **Make it hurt**
  - **Make it less fun, gratifying, profitable…**



Cyber Undercover

- Know your enemy
- Opposition characterization (ala Antionline)
- The more we know about the opposition the better we can protect ourselves
- How are they different
  - Script kiddie
  - Talented amateur
  - Professional
  - Foreign government

Research Project Ideas

- "They got guns, we get guns" (loose quote from *West Side Story*)
  - Translation: make hacker tools available and explain their use.

From an Interview with the Author of *More Guns, Less Crime*

- **“Q: What does the title mean: More Guns, Less Crime?**
- **A: States with the largest increases in gun ownership also have the largest drops in violent crimes. Thirty-one states now have such laws—called "shall-issue" laws. These laws allow adults the right to carry concealed handguns if they do not have a criminal record or a history of significant mental illness.”**
- **http://www.press.uchicago.edu/Misc/Chicago/493636.html**

Hacker Tools

- **If you have used a hacker tool on yourself you are more likely to recognize its use against you**
- **They’re cheap**
- **Some of them are quite good**

Research Project Ideas

- How to make computer security de rigueur for users?
- What can we learn from other efforts?
  - Seat belts
  - DUI
  - Smoking
  - Cholesterol
  - AIDS
  - Lab safety
- We learn slowly, but it can be done with a persistent, consistent message

Messages

- Seat belts
  - Introduced long ago
  - Use encouraged
  - Use made a matter of law
- Safety
  - For years safety at many Labs was good, but not good enough
  - It took management accountability to change attitude and procedures

Research Project Ideas

- Know your enemy
- Use hacker tools
- Learn from other efforts

Conslusion

- Current threats
  - Insider, malicious code, unpatched, passwords, awareness
- Anticipated threats
  - Mobile code and workers, wireless, faster systems
- Countermeasures
  - Communicate, remove hacker advantage
- Research Project Ideas
  - Know enemy, use tools, learn from other efforts